

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

In the Matter of)	
)	
Petition for Expedited Rulemaking to)	RM-11376
Establish Technical Requirements and)	
Standards to Section 107(b) of the)	
Communications Assistance for Law)	
Enforcement Act)	

COMMENTS OF VERIZON WIRELESS

Pursuant to the Commission's May 25, 2007, Public Notice, Verizon Wireless hereby files these comments on the Petition filed by the United States Department of Justice ("DOJ") on May 15, 2007, which asks the Commission to rule that an industry standard is deficient in several respects under the Communications Assistance for Law Enforcement Act ("CALEA").¹

I. SUMMARY

Under Section 107(b) of CALEA, 47 U.S.C. § 1006(b), the Government or any interested party may challenge an industry standard as being non-compliant with the electronic capability requirements set forth in Section 103(a) of CALEA, 47 U.S.C. § 1002(a), and the FCC's rules implementing those provisions. DOJ's Petition requests the Commission to determine that the J-STD-025-B CDMA2000 wireless packet mode standard (the "Standard") is deficient because it does not fully meet the capabilities requirements of Section 103(a). DOJ seeks modifications to the Standard based on its belief that it is deficient or impermissibly vague in the following

¹ *Petition for Expedited Rulemaking to Establish Technical Requirements and Standards Pursuant to Section 107(b) of Communications Assistance for Law Enforcement Act ("CALEA")*, RM-11376 (May 15, 2007) (the "Petition").

respects: (1) the Standard does not require packet reporting on activity; (2) it is vague concerning the requirements for timing information, including time-stamping of packets; (3) it does not require that CDMA carriers provide all reasonably available location information beyond cell site and sector of mobile devices at the beginning and end of call sessions, and specifically seeks latitude and longitude data where available; and (4) it does not provide capabilities that adequately address CALEA's security, performance and reliability requirements.

Verizon Wireless believes that DOJ's proposed revisions to the Standard are either already in place in its network, or are reasonably achievable and can be implemented within DOJ's requested time of 12 months once needed network modifications are made, with one exception. DOJ's request for call identification information ("CII") that will provide latitude and longitude data, beyond the cell site and sector locations already provided to requesting law enforcement agencies ("LEAs"), is not currently reasonably achievable. Network modifications following coordination with vendors are required because the commercial databases and services which access call location at the latitude and longitude level do not currently capture this information for customers that do not dial 911 or subscribe to location based services. Due to the amount of technical development and network reconfigurations that will be required by Verizon Wireless and its vendors, considerable work will need to be done to determine the most effective way to provide this enhanced call location information. Moreover, because providing enhanced call location information will require different software in all of its handsets, Verizon Wireless would need to build this software into new handsets, meaning that the capability cannot be provided absent a complete changeout of the more than 60 million Verizon Wireless handsets that are currently in use. Verizon Wireless believes that the best way to address DOJ's request for enhanced wireless location data is for CDMA carriers and the law enforcement community to

explore ways in which this capability could be developed and what changes to carriers' infrastructure and handsets would need to be made. Verizon Wireless has a long track record of working cooperatively with DOJ and other law enforcement agencies to design and deploy many capabilities in its network to assist LEAs in their lawful surveillance efforts. It stands ready to work with law enforcement in the area of enhanced call location data as well. .

II. ANALYSIS OF REQUESTED CHANGES TO THE STANDARD

The following sections describe DOJ's proposed changes and provide an assessment of Verizon Wireless's capability to achieve and implement the proposed changes to its network and its J-STD-025-B network solution.

A. Packet Reporting Activity

The DOJ requests that the Commission require carriers to provide, as part of CII, the following items: originating IP, terminating IP, IP version, port number extraction, transport layer protocol, and next level protocol. With the exception of port number extraction, all of the requested items are contained within the packet header of an IP packet on Verizon Wireless's network and can be identified and delivered to the CALEA delivery function, and thus provided to LAEs on an individual packet basis or as a summary report.² In order to provide the requested port number information, additional software modifications would be necessary to extract this information from the transport layer of the packet. Based upon its initial evaluation and discussion with its vendors, Verizon Wireless believes this change is reasonably achievable and can be implemented within the 12-month timeframe suggested by DOJ.

² The information contained in a summary report is defined in ATIS 1000013-2007.

B. Time Stamping

The current iteration of J-STD-025-B for packet mode services does not expressly incorporate the timing stamping requirements, which were adopted in the circuit-switched version of the CDMA standard (J-STD-025-A). In an earlier rulemaking addressing the deficiencies of the circuit switched standard for CALEA capabilities,³ the FCC provided guidance that circuit switched intercepts be time-stamped within 200 millisecond accuracy and sent to LEAs within eight seconds of time an intercept begins. Based upon its technical evaluation of its currently deployed capabilities with respect to time-stamping, Verizon Wireless believes the DOJ's request is reasonably achievable, and can be implemented within the 12-month timeframe DOJ suggests.

C. Call Location Information

The DOJ requests that the Standard be changed to require CDMA carriers to provide all "reasonably available CII" for call location information from a mobile handset at the beginning and end of a communication.⁴ The Standard only requires that CALEA compliant packet mode surveillances provide CII for the cell cite and sector for a target's CPE at the beginning and end of an IP call session. Verizon Wireless complies with the existing standard. It also works with law enforcement agencies through manual processes to provide all reasonably available call location information, including more precise location information of its customers in exigent circumstances. This information is provided through triangulation based on cell site and sector information. However, there are only two situations in which the network currently receives

³ *Communications Assistance for Law Enforcement Act, Third Report and Order*, CC Docket No. 97-213, 14 FCC Rcd 13786 (1998) at para. 95-96.

⁴ *See Petition* at 26.

more precise latitude/longitude information from the subscriber's location: when the customer dials 911 and thus triggers Verizon Wireless's handset-based E-911 Phase II GPS solution, and when the customer subscribes to its location-based service and activates the service. Neither situation, however, provides a reasonably achievable capability to deliver this location information to a requesting LEA. Moreover, only a small portion of Verizon Wireless customers activate the location-based service, and existing handsets are not capable of transmitting location information in a manner that would meet DOJ's capability request.

1. Modification of E911 Service

Under Verizon Wireless's handset-based E911 Phase II solution, the GPS chip in the handset communicates with multiple GPS satellites (if those satellites can be "seen" by the handset) and transmits this information to the network, which combines this data with other information for transmission to the appropriate Public Safety Answering Point ("PSAP"). The E911 database does not have location information of the handset that is in use unless and until the customer places an E911 call. Where the location information from the E911 Phase II database is available, it is stored in the E911 database for approximately 30 days.

Verizon Wireless could make network modifications to its E911 and CALEA search functions that could provide latitude and longitude information available for all of its customers, but this would require considerable changes, including the design, installation and testing of a new interface between the E911 database and the CALEA delivery function. In addition, mobile handsets would need to be re-engineered to include a mechanism to allow Verizon Wireless to override a customer's privacy choices and initiate a search for location information on a prospective target's handset. In order to use the ability to initiate or "kick-off" this tracking feature, Verizon Wireless would need to develop and distribute new handsets that incorporate

this location feature. This kick-off feature could be designed to be implemented on a case-by case basis as determined by law enforcement in order to protect the privacy of targets where LEAs do not request enhanced call location information. While these changes are technically feasible, there are no “turn-key” solutions and Verizon Wireless and its vendors would need to develop and implement these changes with the technical assistance of its vendors. Currently the handsets Verizon Wireless sells do not have this capability to self-initiate a search, so it would have to be done prospectively and older handsets could not support it.

Further development with vendors will also be needed to ensure that the latitude and longitude information provided through the proposed reconfiguration of the network will provide a surveillance which meets other capability and security requirements delineated by DOJ. In its Petition, DOJ requests that the Standard be amended to ensure that surveillance is “unobtrusive” and undetectable to the target. One of the major flaws of the above discussed solution is that without any further development and refinements, the target may be able to detect he or she is under surveillance because the handset either slows down or signals that it is being tracked. Therefore, it is very unlikely that a technical solution involving the E911 service meeting all of the capability and security requirements identified by the Petition could be developed and implemented within the timeframe suggested by DOJ.

2. Modification of Existing Location Based Services

Verizon Wireless offers location-based services to customers, which also use GPS technology and provide a source of latitude and longitude information within the current network. These services are provided through a combination of network-based and handset applications that are purchased and activated by customers. For instance, with VZW’s Chaperone or VZNavigator technologies, a customer must purchase a handset that is capable of

providing the service (*i.e.*, “LBS capable handsets”)⁵, affirmatively initiate a software download from Verizon Wireless’s network, and subscribe to this service before the customer can use it. After these activation activities are completed, location based information from GPS can be accessed and stored in Verizon Wireless’s network while the customers is using the service. However, location information is not reported or ascertainable to the network when customers are not using the location based application.

In order to accommodate the privacy choices of its customers, Verizon Wireless has designed its LBS services and capable handsets to allow customers to choose to turn them “on” and “off”. Where a customer has the LBS service turned “off”, the network does not have the capability of tracking that particular handset. In order to include a function that would allow Verizon Wireless, upon receipt of lawful authorization, to override this privacy setting and use LBS capabilities to track the location of a target’s handset, Verizon Wireless will need to design and engineer a new function into its handsets. Current LBS capable handsets do not have this function and thus would not be able to support this feature.

In short, Verizon Wireless could not provide available latitude and longitude information as CII to law enforcement, without redesigning the handset features which are required to send the relevant information to the network, where it can be integrated and provided as part of the packet stream to law enforcement. In order to provision enhanced location data in accordance with DOJ’s request, new handsets would need to be designed to include new software and then marketed to customers. There is no technically feasible way to “push” a software update onto existing handsets to allow Verizon Wireless to self-initiate a search without the customer’s consent or knowledge. Given that Verizon Wireless currently has over 60 million devices in the

⁵ Not all of the handsets Verizon Wireless sells to its customers are capable of providing location-based services. Some handsets that are sold are not capable of providing any of these services. Therefore, existing customers need to buy the proper handsets in order to activate and use these services.

hands of customers, many of which will be relied on for years, the changeout of the entire embedded base of handsets to incorporate a capability to deliver real-time latitude and longitude location to LEAs is not readily achievable under the existing LBS architecture. Substantial time, well beyond the 12-month timeframe DOJ suggests, would be required to develop a solution that would meet the Petition's requirements, and even then the full availability of the solution would need to await subscribers' replacement of their existing handsets.

D. Security, Performance and Reliability

The DOJ's Petition asserts that CDMA carriers should be required to deploy additional security, performance and reliability measures that can quantify packet loss or bit error rates for packet mode surveillances. The DOJ is concerned that without specific requirements to guard against packet loss, the Standard will not adequately ensure that the complete packet data stream is delivered to law enforcement. In order to redress this issue, the DOJ suggests two alternative methods.⁶ The first would be to allow law enforcement to collocate their collection functions at the site of a carrier's delivery function. In the alternative, the DOJ requests that a carrier ensure performance reliability by providing "buffering" and retrieval of packet data over secure VPN facilities.

With respect to the first alternative, Verizon Wireless does not have adequate physical space to accommodate each law enforcement agency's request to collocate equipment where a carrier's delivery functions are housed, and thus does not support the adoption of a collocation capability requirement. However, Verizon Wireless is ready and willing to work with DOJ and other LEAs to explore other methods of providing reliability of data that would be reasonably achievable. Although it is not clear that the Commission can find the Standard deficient under

⁶ *Petition* at 49 n. 110.

CALEA because it does not contain a buffering requirement, Verizon Wireless understands DOJ's goal is to have performance and reliability measures in place that would help it determine when packets are lost, rather than to impose any particular method of accomplishing this goal. Thus, the Petition identifies buffering as one suggested method. Verizon Wireless believes that, through discussions among CDMA carriers and LEAs, other solutions can be identified and considered as well that would address DOJ's goal. These solutions can then be included in modifications to the Standard or implemented by carriers.

Verizon Wireless believes it currently meets or exceeds the other performance reliability and security requirements addressed in DOJ's Petition. Specifically, Verizon Wireless's current security and operating procedures⁷ meet the following criteria DOJ identifies:

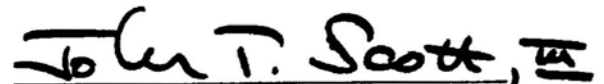
- The capability to ensure that LAEs is "unobtrusive" transparent to and undetectable by the intercept subject, associates and other parties to the communication;
- The capability to prevent unauthorized communications and CII from being intercepted;
- The capability to protect assistance capabilities used to facilitate LAEs;
- Capabilities to protect the confidentiality of LAEs activities (e.g., preventing knowledge of the fact that LAES is being conducted, technical security mechanisms for activating/deactivating LAEs or accessing captured CII or communications content, preventing LAEs subjects from being notified of service changes caused by LAEs; and
- The capability to protect (Securely Deliver) the packet streams as they are delivered to law enforcement.

⁷ A copy of Verizon Wireless's current system security and integrity plan is on file with the FCC in accordance with the requirements of section 105 of CALEA, 47 U.S.C. § 1004.

III. CONCLUSION

Verizon Wireless believes that DOJ's proposed revisions to the Standard are already in place in its network, or are reasonably achievable and can be implemented within DOJ's requested 12-month time frame, except for DOJ's request that it provide enhanced call location information. Due to the technical limitations of commercially deployed location based services and E911 Phase II services, a solution for the delivery of enhanced call location information to include latitude and longitude, as the Petition seeks, is not currently achievable and will take considerably more time to develop and implement than the 12 months suggested by the DOJ. Until a solution exists, Verizon Wireless will continue to provide all reasonably available call location information to LEAs pursuant to lawful intercept requests.

Respectfully submitted,

A handwritten signature in black ink that reads "John T. Scott, III". The signature is written in a cursive style with a horizontal line underneath the name.

John T. Scott, III
Vice President and
Deputy General - Regulatory Law

Elaine Critides, Counsel

VERIZON WIRELESS

1300 I Street, N.W., Suite 400-W
Washington, DC 20005
(202) 589-3740

July 25, 2007

CERTIFICATE OF SERVICE

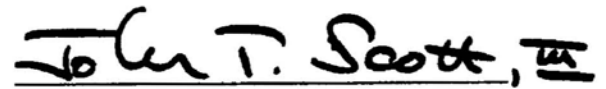
I hereby certify that copies of the foregoing "Comments of Verizon Wireless" were sent
by first-class mail, postage prepaid, to the following:

Sigal P. Mandelker
Deputy Assistant Attorney General, Criminal Division
United State Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530

Elaine N. Lammert
Deputy Attorney General, Office of the General Counsel
Federal Bureau of Investigation
United States Department of Justice

Charles M. Steele
Chief of Staff, National Security Deivsiion
United States Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, D.C 20530

Michael L. Ciminelli
Deputy Chief Counsel
Drug Enforcement Administration
United States Department of Justice
Washington, D.C. 20537


John T. Scott, III